We claim:

1. A method in a computer system for PKI-enabling an application, the method comprising:

integrating the application with an application-specific certification authority for issuing application-specific certificates;

receiving notice of a master certification authority issuing a master certificate to a subscriber; and

issuing to the subscriber an application-specific certificate corresponding to the master certificate, the application-specific certificate for use by the application.

2. The method of claim 1, further comprising:

integrating the application with a directory service for providing access to application-specific certificates for the application.

3. The method of claim 2, wherein the directory service comprises one of a lightweight directory access protocol (LDAP) service, an X.500 directory, and a database.

4. The method of claim 2, wherein the directory service comprises a certificate repository, and wherein issuing comprises:

storing the application-specific certificate in the certificate repository of the directory service.

5. The method of claim 1, further comprising:

receiving notice of the master certification authority revoking the master certificate of the subscriber; and

revoking the application-specific certificate of the subscriber corresponding to the revoked master certificate.

6. The method of claim 5, wherein revoking comprises:

storing an indication of the revoked application-specific certificate in a certificate revocation list.

7. The method of claim 1, further comprising:

integrating the application with a registration authority for registering subscribers and revoking subscribers' certificates;

in response to a subscriber being registered, issuing an application-specific certificate to the subscriber; and

in response to a subscriber's certificate being revoked, revoking the application-specific certificate of the subscriber.

8. The method of claim 1, wherein the master certificate and the application-specific certificate are each associated with a separate public key and a separate private key, and wherein issuing comprises:

encrypting the private key associated with the application-specific certificate using the public key associated with the master certificate.

9. The method of claim 8, further comprising:

in response to the subscriber successfully authenticating with an authentication service using the master certificate:

decrypting the private key associated with the application-specific certificate using the private key associated with the master certificate; and

authenticating the subscriber for the application using the decrypted private key associated with the application-specific certificate.

10. A method in a computer system for PKI-enabling a plurality of applications, the method comprising:

integrating a first application with a first certification authority for issuing certificates specific to the first application;

integrating a second application with a second certification authority for issuing certificates specific to the second application;

receiving notice of a registration authority registering a subscriber;

issuing a first application-specific certificate to the subscriber using the first certification authority, the first application-specific certificate for use by the first application; and

issuing a second application-specific certificate to the subscriber using the second certification authority, the second application-specific certificate for use by the second application.

11. The method of claim 10, further comprising:

integrating the first application with a first directory service for providing access to application-specific certificates for the first application.

12. The method of claim 11, wherein the first directory service comprises a certificate repository, and wherein issuing a first application-specific certificate comprises:

storing the first application-specific certificate in the certificate repository of the first directory service.

13. The method of claim 10, further comprising:

receiving notice of the registration authority revoking a certificate of the subscriber;

revoking the first application-specific certificate of the subscriber using the first certification authority; and

revoking the second application-specific certificate of the subscriber using the second certification authority.

14. The method of claim 13, wherein revoking the first application-specific certificate comprises:

storing an indication of the revoked application-specific certificate in a certificate revocation list.

15. The method of claim 10, further comprising:

integrating the first application with an application-specific registration authority for registering subscribers; and

in response to a subscriber being registered by the application-specific registration authority, issuing an application-specific certificate to the subscriber using the first certification authority.

16. The method of claim 11, further comprising:

integrating the second application with a second directory service for providing access to application-specific certificates for the second application.

17. The method of claim 16, wherein the second directory service comprises a certificate repository, and wherein issuing the second application-specific certificate comprises:

storing the second application-specific certificate in the certificate repository of the second directory service.

18. The method of claim 10, further comprising:

integrating the second application with an application-specific registration authority for registering subscribers; and

in response to a subscriber being registered by the application-specific registration authority, issuing an application-specific certificate to the subscriber using the second certification authority.

19. A method in a computer system for PKI-enabling a plurality of applications, the method comprising:

integrating each of a plurality of applications with an application-specific certification authority, the application-specific certification authority for issuing application-specific certificates;

receiving notice of a registration authority registering subscribers; and

issuing a corresponding application-specific certificate to each subscriber registered by the registration authority.

20. The method of claim 19, further comprising:

receiving notice of the registration authority revoking certificates of one or more subscribers; and

revoking the application-specific certificate of each subscriber for which a corresponding certificate was revoked by the registration authority.

21. A system for PKI-enabling an application, the system comprising:

an application-specific certification authority integrated with the application, the application-specific certification authority configured to issue an application-specific certificate to a subscriber in response to receiving notice of a master certification authority issuing a master certificate to the subscriber, the application-specific certificate for authenticating the subscriber for the application; and

a directory service integrated with the application and configured to provide access to application-specific certificates for the application.

22. The system of claim 21, wherein the directory service comprises one of a lightweight directory access protocol (LDAP) service, an X.500 directory, and a database.

23. The system of claim 21, wherein the directory service comprises a certificate repository for storing certificates specific to the application.

24. The system of claim 21, wherein the application-specific certification authority is further configured to revoke the subscriber's application-specific certificate in response to receiving notice of the master certification authority revoking the master certificate of the subscriber.

25. The system of claim 24, wherein the directory service comprises a certificate revocation list for storing an indication of the revoked application-specific certificate.

26. The system of claim 21, further comprising:

an application-specific registration authority integrated with the application for registering subscribers and, in response to a subscriber being registered, instructing the first certification authority to issue an application-specific certificate to the subscriber, and, in response to a subscriber's certificate being revoked, instructing the first certification authority to revoke the application-specific certificate of the subscriber.

27. The system of claim 21, wherein the master certificate and application-specific certificate are each associated with a separate public key and a separate private key, the system further comprising:

an encryption module configured to encrypt the private key associated with the application-specific certificate using the public key associated with the master certificate.

28. The system of claim 27, further comprising:

a decryption module configured to decrypt the private key associated with the application-specific certificate using the private key associated with the master certificate in response to a subscriber successfully authenticating with an authentication service of the master certification authority using the master certificate and corresponding private key; and

an authentication module configured to authenticate a subscriber for the application using the decrypted private key associated with the application-specific certificate.

29. A system for PKI-enabling a plurality of applications, the system comprising:

a first certification authority integrated with a first application, the first certification authority for issuing a first application-specific certificate to a subscriber in response to receiving notice of a registration authority registering the subscriber, the first application-specific certificate for use by the first application; and

a second certification authority integrated with a second application, the second certification authority for issuing a second application-specific certificate to a subscriber in response to receiving notice of the registration authority registering the subscriber, the second application-specific certificate for use by the second application.

30. The system of claim 29, further comprising:

a first directory service integrated with the first application for providing access to application-specific certificates for the first application.

31. The system of claim 30, wherein the first directory service comprises a certificate repository for storing certificates specific to the first application.

32. The system of claim 29, wherein the first certification authority is further configured to revoke the first application-specific certificate of the subscriber in response to receiving notice of the registration authority revoking a certificate of the subscriber.

33. The system of claim 32, further comprising:

a first directory service integrated with the first application for providing access to application-specific certificates for the first application, wherein the first

directory service comprises a certificate revocation list for storing an indication of the revoked application-specific certificate.

34. The system of claim 29, further comprising:

an application-specific registration authority integrated with the first application for registering a subscriber and, in response to the subscriber being registered, instructing the first certification authority to issue an application-specific certificate to the subscriber.

35. The system of claim 30, further comprising:

a second directory service integrated with the second application for providing access to application-specific certificates for the second application.

36. The system of claim 29, wherein the second certification authority is further configured to revoke the second application-specific certificate of the subscriber in response receiving notice of the registration authority revoking a certificate of the subscriber.

37. The system of claim 36, further comprising:

a second directory service integrated with the second application for providing access to application-specific certificates for the second application, wherein the second directory service comprises a certificate revocation list for storing an indication of the revoked application-specific certificate.

38. The system of claim 29, further comprising:

an application-specific registration authority integrated with the second application for registering subscribers and, in response to a subscriber being

registered, instructing the second certification authority to issue an application-specific certificate to the subscriber.

39. A system for PKI-enabling a plurality of applications, the system comprising:

an application-specific certification authority integrated with each application, the application-specific certification authority for issuing application-specific certificates;

a registration monitoring component integrated with each application-specific certification authority, the registration monitoring component for receiving notice from a registration authority of registration of subscribers; and

a certificate issuance component integrated with each application-specific certification authority, the certificate issuance component for issuing an application-specific certificate to each subscriber registered by the registration authority.

40. The system of claim 39, further comprising:

a revocation monitoring component integrated with each application-specific certification authority, the revocation monitoring component for receiving notice from a registration authority of revocation of subscribers' certificates; and

a certificate revocation component integrated with each application-specific certification authority, the certificate revocation component for revoking the application-specific certificate of each subscriber for which a certificate is revoked by the registration authority.

41. A computer program product for PKI-enabling an application, the computer program product comprising:

program code for integrating the application with an application-specific certification authority for issuing application-specific certificates;

program code for receiving notice of a master certification authority issuing a master certificate to a subscriber; and

program code for issuing to the subscriber an application-specific certificate corresponding to the master certificate, the application-specific certificate for use by the application.

42. The computer program product of claim 41, further comprising:

program code for integrating the application with a directory service for providing access to application-specific certificates for the application.

43. The computer program product of claim 42, wherein the directory service comprises one of a lightweight directory access protocol (LDAP) service, an X.500 directory, and a database.

44. The computer program product of claim 42, wherein the directory service comprises a certificate repository, and wherein issuing comprises:

program code for storing the application-specific certificate in the certificate repository of the directory service.

45. The computer program product of claim 41, further comprising:

program code for receiving notice of the master certification authority revoking the master certificate of the subscriber; and

program code for revoking the application-specific certificate of the subscriber corresponding to the revoked master certificate.

46. The computer program product of claim 45, wherein revoking comprises:

program code for storing an indication of the revoked application-specific certificate in a certificate revocation list.

47. The computer program product of claim 41, further comprising:

program code integrating the application with a registration authority for registering subscribers and revoking subscribers' certificates;

program code for, in response to a subscriber being registered, issuing an application-specific certificate to the subscriber; and

program code for, in response to a subscriber's certificate being revoked, revoking the application-specific certificate of the subscriber.

48. The computer program product of claim 41, wherein the master certificate and the application-specific certificate are each associated with a separate public key and a separate private key, and wherein issuing comprises:

program code for encrypting the private key associated with the application-specific certificate using the public key associated with the master certificate.

49. The computer program product of claim 48, further comprising:

program code for, in response to the subscriber successfully authenticating with an authentication service using the master certificate:

program code for decrypting the private key associated with the application-specific certificate using the private key associated with the master certificate; and

program code for authenticating the subscriber for the application using the decrypted private key associated with the application-specific certificate.

50. A computer program product for PKI-enabling a plurality of applications, the computer program product comprising:

program code for integrating a first application with a first certification authority for issuing certificates specific to the first application;

program code for integrating a second application with a second certification authority for issuing certificates specific to the second application;

program code for receiving notice of a registration authority registering a subscriber;

program code for issuing a first application-specific certificate to the subscriber using the first certification authority, the first application-specific certificate for use by the first application; and

program code for issuing a second application-specific certificate to the subscriber using the second certification authority, the second application-specific certificate for use by the second application.

51. The computer program product of claim 50, further comprising:

program code for integrating the first application with a first directory service for providing access to application-specific certificates for the first application.

52. The computer program product of claim 51, wherein the first directory service comprises a certificate repository, and wherein issuing a first application-specific certificate comprises:

program code for storing the first application-specific certificate in the certificate repository of the first directory service.

53. The computer program product of claim 50, further comprising:

program code for receiving notice of the registration authority revoking a certificate of the subscriber;

program code for revoking the first application-specific certificate of the subscriber using the first certification authority; and

program code for revoking the second application-specific certificate of the subscriber using the second certification authority.

54. The computer program product of claim 53, wherein revoking the first application-specific certificate comprises:

program code for storing an indication of the revoked application-specific certificate in a certificate revocation list.

55. The computer program product of claim 50, further comprising:

program code for integrating the first application with an application-specific registration authority for registering subscribers; and

program code for, in response to a subscriber being registered by the application-specific registration authority, issuing an application-specific certificate to the subscriber using the first certification authority.

56. The computer program product of claim 51, further comprising:

program code for integrating the second application with a second directory service for providing access to application-specific certificates for the second application.

57. The computer program product of claim 56, wherein the second directory service comprises a certificate repository, and wherein issuing the second application-specific certificate comprises:

program code for storing the second application-specific certificate in the certificate repository of the second directory service.

58. The computer program product of claim 50, further comprising:

program code for integrating the second application with an application-specific registration authority for registering subscribers; and

program code for, in response to a subscriber being registered by the application-specific registration authority, issuing an application-specific certificate to the subscriber using the second certification authority.

program code for, in response to a subscriber's certificate being revoked, revoking the application-specific certificate of the subscriber using the second certification authority.

59. A computer program product in a computer system for PKI-enabling a plurality of applications, the computer program product comprising:

program code for integrating each of a plurality of applications with an application-specific certification authority, the application-specific certification authority for issuing application-specific certificates;

program code for receiving notice of a registration authority registering subscribers; and

program code for issuing a corresponding application-specific certificate to each subscriber registered by the registration authority.

60. The computer program product of claim 59, further comprising:

program code for receiving notice of the registration authority revoking certificates of one or more subscribers; and

program code for revoking the application-specific certificate of each subscriber for which a corresponding certificate was revoked by the registration authority.